UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/030,162	04/25/2002	Albert Modl	MODL3003/JEK	4361

23364 7590 06/30/2006

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/030,162	MODL ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9 are pending.

2. The amendment of 3/14/06 has been received and entered.

Response to Arguments

3. The Applicant has argued the following:

(paragraph 5, page 8 – paragraph 1, page 9)

It is respectfully submitted that Boerbert fails to disclose or suggest each and every element set forth in claim 1 of the present application. Boerbert fails to disclose or suggest a method wherein a data carrier terminal reads a secret code from a data carrier,and then presents (displays) the secret code for verification by the user, and then, only upon an indication by the user that the secret code is correct reads biometric data of a biometric feature presented by the user.

Instead Boerbert discloses a method related to security in communication between a computer and a terminal. Such security is obtained by means of a user token. The user presents the token to reading device and is asked to present a PIN. Next, a controller builds a message containing the PIN, the name of the user, an access authorization, and a "last countersign" This message is sent to the computer, which verifies the message. In the PIN or "last countersign" are not as expected, the user is not authorized for use of the computer. However, there is no

teaching or suggestion that the PIN is presented to the user for verification prior to a subsequent step for authenticating the user based on a biometric feature.

The Examiner contends however that the Applicant's claim does not explicitly recite that the PIN presented to the user should then be submitted to a subsequent step for authenticating the user based on a biometric feature. The claim recites

- After receiving an indication that the presented read secret code is correct, reading a biometric feature presented by the user.

However, it is the Examiner's interpretation of the claim that whether the code is first presented or not is not explicitly stated by the claim. It is only clearly indicated in the claim recited that

1) an indication of the secret code is correct

2) that the read secret code is "presented" at all.

That is to say, it is the Examiner's interpretation that even if the read secret code is "presented after" a biometric feature is read, that code may still properly be referred to as "the presented read secret code" within the recitation of the claim.

Applicant has further argued on paragraph 2, page 10:

It is respectfully submitted that Boerbert fails to disclose or suggest that a secret code is stored on the user identity token in a manner such that the secret code can be read only by an authorized data carrier terminal.

The Examiner contends though that one of ordinary skill in the art would interpret the Boerbert has implicitly meeting this limitation. (Column 7, lines 52 – Column 8, line 2) & (Column 11, lines 1-11) recites that the data transmitted between the user and the computer are encrypted. Thus only computers with the means of decrypting the data are capable of reading the data.

Applicant has further argued on paragraph 5, page 10:

Further, there is no specific teaching or suggestion that the biometric data is used in addition to, rather than instead of, the PIN number stored on the user identity token. Therefore, there is no teaching or suggestion of 1) biometric data stored in a data carrier; or 2) a data carrier having a first memory area for storing a secret code and a second memory area for storing biometric data; or 3) a data carrier terminal that has both a device for reading the secret code and a device for reading biometric data.

The Examiner contends however that the read biometric data of (Column 7, lines 40-46) recites that "user authentication device could *include* a biometric device for determining a unique physical attribute of a user..." and that "that data would then be sent to computer 60 during the user verification process described in Figure 4." For this reason, the Examiner contends that the biometric information could be used in addition to the PIN of Figure 4. Finally, the Examiner respectfully disagrees with the Applicants contentions and deductions that there is no teaching or suggestion of biometric data stored in a data carrier. Column 7, lines 40-46 clearly states that the biometric data such as fingerprints or palm prints is sent to computer 60 during the process of

figure 4. This "sending" of the biometric data teaches and at least suggests that biometric data is stored in a data carrier—namely the carrier that will send the data to computer 60.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boerbert, US patent 5,272,754.

In reference to claim 1:

Boerbert discloses a method for authenticating a user of a data carrier for authorized use of the data carrier and for authenticating a data carrier terminal for authorized accessing by the data carrier terminal of memory areas of the data sheet carrier (Column 2, lines 17-24, 37-45), comprising the following steps:

- Reading a secret code from the data carrier by the data carrier terminal, wherein the secret code is stored on a memory location that can be accessed only by authorized data terminals or can be decrypted correctly, where the code is the token information. (Figure 4, Items 100, 102), and where the token information is read by the terminal and decrypted

(Column 5, lines 10-26) & (Column 4, line 48 – Column 5, line 11) & (Column 7, line 52 – Column 8, line 2)

- Presenting the read secret code to the user, where the code presented is the token information which is the countersign. (Column 11, lines 3-11)
- After receiving an indication that the presented read secret code is correct, reading a biometric feature presented by the user. (Column 7, lines 40-46)

Boerbert fails to explicitly disclose

- Comparing the presented biometric feature with a biometric feature stored on the data carrier.

Boerbert however discloses that in an alternate embodiment, the user authentication device can include a biometric device, which would then be sent to a computer during the user verification process described in Fig 4. (Column 7, lines 40-46)

It is shown in Figure 4, that the invention of Boerbert verifies the authentication information at Items 114. (Column 10, lines 1-10) discloses the computer 60 checks the authentication information for correctness.

It would have been obvious to one of ordinary skill in the art to compare the presented biometric information in order to verify it in order to authenticate the user based on biometric information.

In reference to claim 2:

Boerbert (Column 9, line 57 – Column 10, line 11) discloses a method according to claim 1, further comprising a step wherein a PIN is in addition presented to the terminal, being compared with a PIN stored on the data carrier.

In reference to claim 3:

Boerbert (Column 7, lines 40-46) discloses a method according to claim 1 or claim 2, wherein a fingerprint of a user is used as the biometric feature.

In reference to claim 4:

Boerbert discloses a data carrier for authenticating a user of the data carrier and for authenticating a data carrier terminal for accessing the data carrier (Column 2, lines 17-24, 37-45) & Figure 4, comprising a first memory area in which a secret code(CODE) is stored such that the secret code can be read and decrypted and displayed only by an authorized data carrier terminal to authenticate the data carrier terminal for accessing the data carrier (Column 5, lines 10-26) & (Column 4, line 48 – Column 5, line 11) & (Column 7, line 52 – Column 8, line 2), and a second memory area in which data are stored which serve to authenticate the user for authorized use of the data carrier. (Figure 2) & (Figure 4, Item 114) & (Column 5, lines 10-25)

In reference to claim 5:

Boerbert (Column 9, line 57 – Column 10, line 11) discloses a data carrier according to claim 4, wherein a PIN is stored in a third memory area.

In reference to claim 6:

Boerbert (Column 7, lines 40-46) discloses a data carrier according to either of claims 4 and 5, wherein the biometric data are generated by a fingerprint.

In reference to claim 7:

An authentication system comprising a data carrier with memory areas and a data carrier terminal for accessing the memory areas of the data carrier, wherein

- The data carrier has a first memory area for storing a secret code (Column 5, lines 10-25) and a second memory area for storing biometric data. (Column 7, lines 40-46)
- The data carrier terminal has a first device which is authorized for reading the secret code from the first memory area and for decrypting the read secret code and for presenting the read secret code on a display, where the code is the token information. (Figure 4, Items 100, 102), and where the token information is read by the terminal and decrypted (Column 5, lines 10-26) & (Column 4, line 48 – Column 5, line 11) & (Column 7, line 52 – Column 8, line 2),

Boerbert fails to explicitly disclose

- A device for comparing the read biometric data (BIO) with biometric data stored in the second memory area in the data carrier (C) and/or in the terminal (T).
- and a second device for reading biometric data (BIO) of a biometric feature presented by a user.

Boerbert however discloses that in an alternate embodiment, the user authentication device can include a biometric device, which would then be sent to a computer during the user verification process described in Fig 4. (Column 7, lines 40-46)

It is shown in Figure 4, that the invention of Boerbert verifies the authentication information at Items 114. (Column 10, lines 1-10) discloses the computer 60 checks the authentication information for correctness.

It would have been obvious to one of ordinary skill in the art to compare the presented biometric information in order to verify it in order to authenticate the user based on biometric information.

In reference to claim 8:

Boerbert (Column 9, line 57 – Column 10, line 11) discloses an authentication system according to claim 7, wherein the data carrier has a third memory area for storing a PIN.

In reference to claim 9:

Boerbert (Column 7, lines 40-46) discloses an authentication system according to claim 7 or 8, wherein the stored biometric data are generated by a fingerprint.

Conclusion

6. The following art not relied upon is made of record:

- US patent 5930804 discloses an online biometric system with server client authentication.

- US patent, 6424249 discloses a biometric recognition system for identifying a user.

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571)272-6962.
The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

June 20th, 2006

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER